Please amend the present application as follows:

Claims

The following is a copy of Applicant's claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("~~—~~"), as is applicable:

1. (Currently amended) A method for securely transmitting data between a computer and a printer, comprising:

converting a file for printing into a printer description language format;

encrypting said file in said printer description language format;

adding an unencrypted header to said encrypted file;

providing ~~said file with~~ an identifier in ~~a~~ said header ~~of said file~~ that provides an indication of an algorithm that was used to encrypt said file; and

transmitting said file and header to the printer.

2. (Original) The method of claim 1, further comprising decrypting said file by the printer.

3. (Previously presented) The method of claim 1, wherein said converting comprises converting said file into at least one of a postscript format, a PCL format, a PDF format, and an XML format.

4. (Previously presented) The method of claim 1, further comprising: receiving said file by the printer, the printer recognizing said identifier, validating said identifier, and selecting an appropriate decryption algorithm that is associated with the computer.

5. (Previously presented) The method of claim 1, wherein said providing includes providing said header of said file with a flag recognizable solely by the printer for identifying an encryption algorithm used in said encrypting.

6. (Canceled)

7. (Previously presented) The method of claim 5, further comprising recognizing said flag with the printer and selecting an appropriate decryption algorithm.

8. (Previously presented) The method of claim 7, further comprising validating said flag on the printer by entering a decryption key into the printer that corresponds to said flag.

9. (Canceled)

10. (Previously presented) The method of claim 7, wherein selecting an appropriate decryption algorithm comprises selecting an appropriate decryption algorithm from a plurality of decryption algorithms available to the printer.

11. (Currently amended) A method for securely transmitting data between a first device and a second device in a computer network, comprising:

encrypting a file to be transmitted by the first device;

adding an unencrypted header to said encrypted file;

providing ~~a header of said file with~~ an identifier in said header that provides an indication of an algorithm that was used to encrypt said file; and

transmitting said file and header from the first device to the second device.

12. (Original) The method of claim 11, further comprising:

decrypting said file by the second device.

13. (Previously presented) The method of claim 12, wherein encrypting comprises encrypting said file by employing one of a plurality of encryption programs available to the first device and further comprising performing on the second device prior to decrypting at least one of recognizing said identifier, validating said identifier, and selecting an appropriate decryption algorithm from a plurality of decryption algorithms.

14. (Previously presented) The method of claim 13, wherein said providing includes providing a flag in said header of said file, said flag recognizable only by the second device and identifying which of said plurality of encryption programs was used to encrypt said file.

15. (Canceled)

16. (Previously presented) The method of claim 14, further comprising performing with the second device at least one of recognizing said flag, validating said flag using a decryption key corresponding to said flag of the second device, and selecting an appropriate decryption algorithm from said plurality of decryption algorithms.

17. (Currently amended) A system for securely transmitting a file in a computer network, comprising:

a first device including at least one processor for providing an encrypted file with an unencrypted header that includes an identifier that provides an indication as to an encryption algorithm that was used to encrypt the file; and

a second device including at least one processor for decrypting and outputting the file.

18. (Previously presented) The system of claim 17, wherein said first device includes at least one encryption algorithm.

19. (Previously presented) The system of claim 18, wherein said at least one processor of said first device is configured to provide the file header with a flag that identifies an encryption algorithm that was used to encrypt the file.

20. (Previously presented) The system of claim 19, wherein said second device further includes an input element for entry of a decryption key for recognition by said at least one processor of said second device and for corresponding to at least one decryption algorithm available to said at least one processor of said second device and said flag accompanying the file.

21. (Previously presented) The system of claim 17, wherein said first device comprises a computer and said second device comprises a printer, said first device having apparatus for converting the file into a printer description language format.

22. (Previously presented) The system of claim 17, wherein said first device includes at least one encryption algorithm that corresponds to a decryption algorithm available to said second device.

23. (Currently amended) A printer, comprising:

at least one processor configured to receive an encrypted file for printing and configured to read an identifier provided in an unencrypted header ~~of~~ associated with said encrypted file, the identifier providing an indication of an encryption algorithm that was used to encrypt said file, said at least one processor being configured to execute a decryption algorithm to decrypt said encrypted file; and

at least one printing element for printing said file.

24. (Original) The printer of claim 23, further comprising a memory connected to said at least one processor for storage of said decryption algorithm.

25. (Original) The printer of claim 23, further comprising:

at least one decryption algorithm associated with said at least one processor.

26. (Previously presented) The printer of claim 23, wherein said identifier identifies at least one of the source of said encrypted file and a an encryption algorithm that was used to encrypt said encrypted file.

27. (Previously presented) The printer of claim 26, wherein said at least one processor selects a decryption algorithm for decrypting said encrypted file from a plurality of available decryption algorithms based upon said identifier.

28. (Previously presented) The printer of claim 26, further comprising an input element configured for receiving decryption key, said decryption key corresponding to said identifier.

29. (Original) The printer of claim 28, wherein said decryption key facilitates activation of a decryption algorithm.